DRAFT
DOE M 205.1-C

Approved: XX-XX-03
Sunset Review: XX-XX-05
Expires: XX-XX-07

INCIDENT PREVENTION, WARNING, AND RESPONSE (IPWAR) MANUAL

U.S. DEPARTMENT OF ENERGY
Office of the Chief Information Officer

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Office of the Chief Information Officer

INCIDENT PREVENTION, WARNING, AND RESPONSE (IPWAR) MANUAL

1. OBJECTIVES.

   a. To provide requirements and implementation instructions for the Department of Energy (DOE) incident prevention, warning, and response (IPWAR) process to supplement DOE O 205.1, *Department of Energy Cyber Security Management Program,* 3-21-03.

   b. To assist the Department and Departmental elements in:

      (1) preparing for, preventing, warning of, and recovering from cyber security incidents through the timely sharing of information regarding vulnerabilities, threats, attempted and successful exploits, and other anomalous activities;

      (2) identifying the roles and responsibilities necessary to promote an effective Department-wide IPWAR capability;

      (3) developing appropriate local IPWAR procedures;

      (4) standardizing reporting procedures to improve timeliness, increase clarity, support effective analysis, and ensure consistency with and provide necessary support to Government-wide requirements and capabilities; and

      (5) measuring the performance of Departmental IPWAR capabilities to promote a process of continuing improvement.

   c. To ensure the Department meets the requirements of Federal laws, Executive Orders, national security directives, and other regulations.

2. CANCELLATIONS. DOE N 205.4, *Handling Cyber Security Alerts and Advisories and Reporting Cyber Security Incidents,* 3-18-02.

3. APPLICABILITY.

   a. DOE Elements. Except for the exclusions in paragraph 3c, this Manual applies to all DOE Programs and elements, including National Nuclear Security Administration programs and elements, that own or operate Federal information systems or National security systems (see Attachment 1).

   b. Site/Facility Management Contractors.

      (1) Except for the exclusions in paragraph 3c, the Contractor Requirements Document (CRD), Attachment 2, sets forth the requirements of this Manual that will apply to those site/facility management contractors whose contracts include the CRD.

(2) This CRD must be included in all site/facility management contracts that require or involve access to DOE information systems.

(3) This CRD does not automatically apply to other than site/facility management contractors. Any application of any requirements of this Manual to other than site/facility management contractors will be communicated separately from this Manual.

(4) The Heads of Departmental elements are responsible for notifying contracting officers of which site/facility management contractors are affected by this Manual (see Attachment 3). Once notified, contracting officers are responsible for incorporating the CRD into each affected site/facility management contract via the laws, regulations, and DOE Directives clause of the contract.

(5) As the laws, regulations, and DOE Directives clause of site/facility management contracts states, regardless of who performs the work, site/facility management contractors with a CRD incorporated into their contracts are responsible for complying with the requirements of the CRD. Affected site/facility management contractors are responsible for flowing down the requirements of this CRD to subcontracts at any tier to the extent necessary to ensure the site/facility management contractors' compliance with the requirements. In doing so, they must not unnecessarily or imprudently flow down requirements to subcontractors. That is, contractors will (a) ensure that they and their subcontractors comply with the requirements of this CRD and (b) only incur costs that would be incurred by a prudent person in the conduct of competitive business.

c. Exclusions. Consistent with the responsibilities identified in Executive Order 12344, the Director of the Naval Nuclear Propulsion Program will ensure consistency through the joint Navy and DOE organization of the Naval Nuclear Propulsion Program and will implement and oversee all requirements and practices pertaining to this DOE Manual for activities under the Deputy Administrator's cognizance.

4. SUMMARY.

All Departmental elements that own, operate, or have access to Federal information systems or national security systems must report cyber security incidents to the Computer Incident Advisory Capability (CIAC) and other Departmental organizations in accordance with the guidance in this Manual. CIAC will then pass the incident information on to the Federal Computer Incident Response Center (FedCIRC) as required by Federal legislation and Executive requirements. This document outlines procedures that will improve and measure the performance of the Department's capabilities to prepare for, prevent, warn of, respond to, and recover from cyber incidents.

Chapter I gives background information and outlines requirements, Chapter II lists the responsible officers and their responsibilities, Attachment 1 lists the DOE organizations to which this Manual applies, Attachment 2 is the Contractor Requirements Document (CRD), and Attachment 3 lists the current contractors to which the Manual's CRD applies. Attachment 4 defines terms used in this Manual, Attachment 5, identifies acronyms used, and Attachment 6 is a sample cyber incident response plan. Attachment 7 is a sample incident recognition and reporting worksheet.

5. IMPLEMENTATION.

Heads of Departmental elements must implement the responsibilities and requirements contained in this Manual within 180 days of its issuance. Contractors who provide direct support to Departmental elements will report through appropriate levels of Departmental element management.

6. REFERENCES.

The following public laws and policies contain cyber security program requirements and guidance that may be helpful in implementing this Manual.

a. Public Law (P.L.) 107-347, *E-Government Act of 2002, Title III—Information Security* (also known as the Federal Information Security Management Act of 2002), December 2002.

b. Computer Fraud and Abuse Act of 1986, Title 18 U.S.C., Section 1030, Fraud and Related Activity in Connection with Computers.

c. Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, Appendix III, "Security of Federal Automated Information Resources," November 28, 2000.

d. OMB Memorandum, "Improved FedCIRC Incident Reporting System," from Mark Forman, OMB Associate Director for Information Technology and Electronic Government, to Chief Information Officers, November 14, 2003.

The following national standards and guidelines provide relevant processes and procedures for implementing this manual.

a. National Institute for Standards and Technology (NIST) Special Publication (SP) 800-3, *Establishing a Computer Security Incident Response Capability,* November 1991.

b. NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook,* October 1995.

c. NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems,* December 1998.

The following DOE directives provide relevant requirements and procedures for implementing this manual.

a. DOE O 205.1, *Department of Energy Cyber Security Management Program*, 3-21-03.

b. DOE O 221.1, *Reporting Fraud, Waste, and Abuse to the Office of Inspector General,* 3-22-01.

c. DOE O 5670.3, *Counterintelligence Program*, 9-4-92.

d. DOE N 221.8, *Reporting Fraud, Waste, and Abuse,* 7-29-02.

e. DOE N 471.3, *Reporting Incidents of Security Concern*, 4-13-01

f. DOE P 205.1, *Departmental Cyber Security Management Policy*, 5-8-01.

7. CONTACT. Questions concerning this Manual should be addressed to the Office of the Chief Information Officer, 202-586-0166.

BY ORDER OF THE SECRETARY OF ENERGY:

KYLE E. McSLARROW
Deputy Secretary

CONTENTS

CHAPTER I. CYBER SECURITY INCIDENT REPORTING REQUIREMENTS

1. INTRODUCTION.

The DOE Office of the Associate Chief Information Officer (CIO) for Cyber Security is responsible for Department-wide cyber security policy and developing supporting guidance. This responsibility was established in DOE O 205.1, *Department of Energy Cyber Security Management Program,* 3-21-03. This Manual establishes the framework for the prevention, warning, and response to cyber incidents. The Federal Information Security Management Act of 2002 (FISMA) requires Agencies to develop procedures for detecting, reporting, and responding to security incidents, including mitigating risks associated with incidents before substantial damage is done and notifying and consulting with the Federal Computer Incident Response Center (FedCIRC), law enforcement and Inspectors General, and other offices about incidents involving Federal information systems.

Office of Management and Budget (OMB) policy reminds Agencies of the underlying value of developing and maintaining effective incident detection and reporting programs because "due to the Federal government's internetworked environment, Agency components that fail to detect and report IT (information technology) security incidents will likely cause significant problems throughout the Agency network and may impact other Departments and Agencies."[1] Thus, the OMB memorandum, *Improved FedCIRC Incident Report System* (November 14, 2002), directs Agencies to "report all unauthorized system activity (cyber security incidents) quickly and accurately" to FedCIRC. In addition, in its guidance on fiscal year 2002 reporting under the Government Information Security Reform Act of 2000, OMB directed Agencies to certify in their reports that "both the agency and each of its components have established processes that ensure timely, accurate reporting to FedCIRC on security incidents and where appropriate to law enforcement authorities . . . ."

This Manual establishes the framework for the DOE incident prevention, warning, and response (IPWAR) capability for classified and unclassified cyber systems. Its purpose is to define within DOE the roles, responsibilities, and processes for Department-wide proactive analysis and corrective actions to mitigate or reduce the occurrence of cyber security incidents. In addition, the Manual ensures that this aspect of the DOE Cyber Security Management Program (CSMP) meets the requirements of Federal laws, Executive Orders, national security directives, and other regulations.

2. REQUIREMENTS.

a. Categorizing Cyber Security Incidents and Attempted Incidents. Cyber security incidents must be characterized and categorized according to their potential to

[1] Policy: Memorandum to Chief Information Officers, OMB CIO, RE: Handling and Reporting Computer Security Incidents, Sept 12, 2002

cause damage to information and information systems based on two criteria: incident type and system category.[2] The criteria are used in combination to determine the time frame for reporting incidents to the Computer Incident Advisory Capability (CIAC). This Manual establishes two incident types (type 1 and type 2) and three categories of system impact (low, moderate, and high), which are described below.

(1) Incident Types.

(a) Type 1 incidents are successful incidents that potentially create serious breaches of DOE cyber security or have the potential to generate high-visibility media interest. Following are the type 1 incidents currently defined (see also Attachment 4, Definitions).

1. *Compromise/Intrusion*. All instances of system compromise or intrusion by unauthorized persons must be reported, including user-level compromises, root (administrator) compromises, and instances in which users exceed privilege levels.

2. *Web Site Defacement*. All instances of a defaced Web site must be reported.

3. *Malicious Code*. All instances of successful infection or persistent attempts at infection by malicious code, such as viruses, Trojan horses, or worms, must be reported.

4. *Denial of Service*. Denial of service (successful or persistent attempts) that affects or threatens to affect a critical service or denies access to all or large portions of a network must be reported. Critical services are determined by the Heads of Departmental elements.

5. *Critical Infrastructure Protection (CIP)*. Any activity that adversely affects an asset classified as CIP must be reported. CIP assets are determined by the Heads of Departmental elements.

(b) Type 2 incidents are attempted incidents that pose potential long-term threats to DOE cyber security interests or that potentially degrade the overall effectiveness of the Department's cyber

[2] The security categorization of systems established by this Manual is based on Federal Information Processing Standards Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, May 2003 (Initial Public Draft).

security posture. Following are the type 2 incidents currently defined.

1. *Attempted Intrusion*. A significant and/or persistent attempted intrusion is an exploit that stands out above the daily noise level and would result in unauthorized access (compromise) if the system were not protected.

2. *Reconnaissance Activity.* Persistent surveillance probes and scans are those that stand out above the daily noise level and represent activity that is designed to collect information about vulnerabilities in a network. Departmental elements must determine the standard for collecting data on surveillance probes and scans by subordinate sites.

3. *Unauthorized Use*. Computer is used for anything but its intended purpose (that is, information is obtained without permission or the system is used to gain access to DOE data without proper permissions).

(2) System Category. System categories refer to the impact that an incident could have on Departmental operations (including mission, functions, image, or reputation), Departmental assets, or individuals (including harm to privacy rights) based on the sensitivity of the system and the data it stores, processes, or transmits. This categorization translates into a level of risk associated with the potential loss of confidentiality, integrity, or availability of the system and/or the data stored, processed, or transmitted by the system.

(a) Low Risk. Loss of system confidentiality, integrity, and availability could be expected to have a limited adverse effect on Departmental operations, assets, or individuals, requiring minor corrective actions or repairs.

(b) Moderate Risk. Loss of system confidentiality, integrity, and availability could be expected to have a serious adverse effect on Departmental operations, assets, or individuals, including significant degradation or major damage, requiring extensive corrective actions or repairs.

(c) High Risk. Loss of system confidentiality, integrity, and availability could be expected to have a severe or catastrophic adverse effect on Departmental operations, assets, or individuals. The incident could cause the loss of mission capabilities for a

period that poses a threat to human life or results in the loss of major assets.

b. Reporting Cyber Security Incidents. Guidelines for determining the type of reporting must be documented in the Departmental element Program Cyber Security Plan (PCSP).

(1) When a cyber security incident has occurred or is suspected to have occurred, the affected site will immediately examine and document the pertinent facts and circumstances surrounding the incident. (Note: The evidence-gathering period must not exceed 24 hours.)

(2) Once the preponderance of evidence indicates an incident has occurred, the incident must be cataloged according to incident type and category of system affected and reported to CIAC within the time frames indicated in Table 1, in accordance with the process established by the Departmental element.

(3) If it is determined that an incident did not occur, no further action is required.

Table 1. Required Time Frame for Reporting Cyber Security Incidents to the Computer Incident Advisory Capability

	System Category		
Incident Type	**Low**	**Moderate**	**High**
Type 1	Within 4 hours	Within 1 hour	Within 1 hour
Type 2	Within 1 week	Within 24 hours	Within 24 hours

(4) The site must issue a monthly report whether or not it has not experienced any reportable successful or attempted cyber security incidents during the previous month. The reporting process documented in the Departmental element's PCSP should be followed. (Must be checked against PCSP requirements to make sure reporting requirement is documented).

(5) Departmental elements or subordinate organizations must inform the Office of Inspector General of attacks or activities (including persistent attempts at unauthorized access, malicious code, and denial-of-service events) if there is reason to suspect that the attacks/activities are significant, if the attacks/activities are unusually persistent, or if the attacks/activities appear to constitute criminal activity. Reporting this

information to the Office of Inspector General must be done according to the procedures in the PCSP of the Departmental element.

(a) A guideline to help determine whether such events are significant can be found at http://cio.doe.gov/cyberhome/sigguideline.htm.

(b) A guideline to help determine whether such events constitute criminal activity can be found at http://cio.doe.gov/cyberhome/crimguideline.htm.

(6) Automated systems may be used for reporting if reporting by such systems complies with the requirements of this Manual.

c. Cyber Alerts.

(1) CIAC is the official DOE point of contact for prompt dissemination of information provided in alerts received from external organizations. In addition, CIAC provides Departmental responses to national centers, as required. The timing of distribution will be commensurate with the significance of the information.

(2) If CIAC issues an alert, the security points of contact will:

(a) acknowledge the receipt of the alert within 4 business hours and

(b) execute the required analyses and corrective actions and report the actions taken in accordance with the Departmental element's PCSP.

d. Updating Cyber Security Patches. Security patches must be installed regularly and in a timely manner to help prevent intrusions. (Patches can be obtained from a number of sources, including CIAC, the FedCIRC Web site, and trusted vendors.)

e. Cyber Security Incident Preparedness/Response and Contingency Plans. Because of the interrelationship of cyber security incident preparedness/response and continuity of operations, IPWAR procedures should be integrated into, and tested periodically with, the Departmental elements' information system contingency plans. Contingency plans should include a description of or reference to the IPWAR procedures that would be followed to ensure that the system will continue to have incident protection if a disaster occurs.

f. Cyber Security Incident Training. Departmental elements must ensure that users, system administrators, and cyber security staff are well-versed in IPWAR procedures through initial and annual refresher computer security awareness training.

CHAPTER II. CYBER SECURITY INCIDENT MANAGEMENT STRUCTURE AND RESPONSIBILITIES

To ensure an effective and proactive approach to incident handling, the Department must plan and act across the incident life cycle. This life-cycle-based methodology requires responsible officers/elements to address their roles and responsibilities before, during, and after an incident has occurred. Therefore, the descriptions of responsibilities in this Manual are presented in the following categories:

- Prepare and Prevent:
- Detect, Respond: and Report.
- Restore and Improve.

1. Office of the Chief Information Officer (OCIO).

   a. Prepare and Prevent.

      (1) Maintains emergency contact information for Federal and contractor cyber security points of contact.

      (2) Provides management and budgetary oversight and guidance to CIAC.

      (3) Provides oversight, coordination, and management for a coherent incident awareness, handling, and training program for all DOE elements.

      (4) Coordinates and provides overall IPWAR security procedure requirements, definitions, and actions.

      (5) Provides standard security banner for users to view upon login defining appropriate use of the system.

   b. Detect, Respond, and Report.

      (1) Establishes organizational approach to incident handling.

      (2) Coordinates reporting to and interaction with OMB, the Federal CIO Council, and other Federal policy officials concerning threats, vulnerabilities, and incidents of Government-wide significance.

      (3) Serves as the primary point of contact and reporting agent on all IPWAR incidents involving the DOE Headquarters site.

   c. Restore and Improve.

(1) Measures the performance of and provides overall policy, management, and compliance oversight for the DOE IPWAR capability.

(2) Disseminates information on cyber security incidents, as appropriate, to Department-level senior management, consistent with agreed-on procedures.

(3) Identifies Departmental and external IPWAR-related methods, and facilitates the sharing of these methods across DOE.

2. Computer Incident Advisory Capability.

a. Prepare and Prevent.

(1) Provides analysis and watch and warning capabilities to prevent cyber security incidents or reduce their impact to the Department.

(2) Correlates data gathered from perimeter scanning with threat and vulnerability alerts to help identify high-risk Departmental elements.

(3) Provides information to Departmental elements in a timely manner when security patches for software used by the Department become available.

(4) Provide computer forensics and evidence-handling assistance to individuals investigating and preserving cyber evidence.

(5) Provides, as requested, incident reporting and information collection aids for use in properly capturing critical information concerning an incident.

b. Detect, Respond, and Report.

(1) Serves as the Department's central cyber incident reporting point of contact for the receipt of alerts, advisories, notices, bulletins, or other cyber security information from external organizations and the receipt of cyber security information from Departmental elements.

(2) Logs all cyber security incident reports, acknowledges receipt, and assigns incident numbers.

(3) Notifies Heads of Departmental elements and subordinate elements in a timely manner, through primary and alternate points of contact, that an alert regarding a threat, vulnerability, and/or associated patch has been posted for their review and action.

(4) Consistent with law and policy, reports all cyber security incidents quickly and accurately to FedCIRC within the Department of Homeland Security. Transmits initial reports of cyber security incidents received from

Departmental elements to the DOE Headquarters Emergency Operations Center, and, as necessary, transmits subsequent reports to the Associate CIO for Cyber Security and the Office of Security. Where appropriate, reports cyber security incidents to law enforcement authorities in coordination with the affected sites.

(5) In coordination with the lead Departmental element, assists the Office of the Associate CIO for Cyber Security in determining whether conditions indicate that a multiple-site event that warrants reporting to the Offices of Inspector General, Counterintelligence, and/or Security has occurred or is developing.

(6) Provides incident response assistance to the Department during an active event, including securing and collecting incident information.

c. Restore and Improve.

(1) When requested, provides Departmental element management with timely and effective technical and nontechnical assistance (tools, methods, and guidance) in response to a cyber security incident.

(2) Provides reports of significant cyber security incidents to the Associate CIO for Cyber Security.

(3) Provides aggregated performance measure data for the Department to the OCIO on an annual and ad hoc basis.

(4) Collaborates with incident response centers in private industry, the Department of Defense, and other Government agencies.

(5) Provides lessons learned, follow up reports, and recommended updates to security methods to Departmental elements to improve the Agency's policies and procedures.

3. Heads of Departmental Elements.

a. Prepare and Prevent.

(1) Establish, within their respective PCSPs, processes and procedures to ensure that the requirements of this Manual are implemented and documented in their subordinate elements' Cyber Security Program Plans (CSPPs) or system security plans.

(2) Provide, keep current, and test emergency contact information for Federal and contractor reporting, and ensure that information is provided to the Office of the Associate CIO for Cyber Security.

(3) Ensure that processes to update security software and patches on regular and emergency bases are established and documented in the Departmental element's PCSP.

(4) Develop a cyber incident response plan, including the scope of the plan, the roles and responsibilities of the Computer Incident Response Team (CIRT), and a formalized set of procedures for reporting and handling information technology security incidents. The computer incident response plan should be included or referenced in the Departmental element's PCSP document (see Attachment 6 for content of a sample plan). The Departmental element and each sub-element should have a response plan or at least a procedure for reporting incidents. Local implementation procedures should be included as part of the CSPP.

(5) Ensure CIRTs include representatives from different offices within the Departmental element who can aid in handling an incident.

(a) The team should include individuals with competencies matching the roles and responsibilities identified in Attachment 6 of this Manual.

(b) Provide materials and/or train team members on their roles in the incident response process.

(6) Include counterintelligence-related responsibilities in their Departmental element's PCSP and ensure compliance with DOE O 5670.3, *Counterintelligence Program,* 9-4-92, for counterintelligence-related events.

(7) In coordination with the OCIO, establish (and document within their Departmental element's PCSPs) a process for reporting incidents to the Technology Crimes Section of the Office of Inspector General, in accordance with DOE O 221.1, *Reporting Fraud, Waste, and Abuse to the Office of Inspector General,* 3-22-01, and DOE N 221.8, *Reporting, Fraud, Waste, and Abuse,* 7-29-02.

(8) Ensure that all users, system administrators, and cyber security staff are provided with awareness training, materials, and checklists regarding IPWAR procedures on an initial and annual basis.

b. Detect, Respond, and Report.

(1) Promote incident reporting within the organization and ensure users understand there will be no retaliation for reporting incidents.

(2) Ensure that a process is established, documented, tested, and included in the PCSP for subordinate elements to report all cyber security incidents to CIAC and, where appropriate, in coordination with CIAC, to law enforcement authorities.

(3) Establish, within their respective Departmental element's PCSPs, processes and procedures to ensure that the requirements of this Manual are implemented and documented in their subordinate elements' CSPPs or system security plans.

(4) Work with CIAC to determine the severity or significance of cyber security incidents, based on the incident type and associated level of risk.

(5) Ensure that a process is established and documented in the PCSP for subordinate elements to report all cyber security incidents (as defined in Chapter I) to the Head of the Departmental element and subordinate organization management and/or the investigating organizations, as appropriate.

(6) Document in their PCSPs processes for handling information disseminated by CIAC, including procedures for responding proactively to alerts, consequence analyses, and corrective actions. Implementing procedures will be documented in their subordinate elements' CSPPs and/or system security plans.

c. Restore and Improve.

(1) Ensure that IPWAR procedures are integrated into and tested periodically with the Departmental element's contingency plan. The contingency plan should include a description of or reference to the IPWAR procedures that would be followed to ensure that the system will continue to have incident protection if a disaster occurs.

(2) Measure the implementation of DOE IPWAR policy requirements within the Departmental element through performance measures.

(3) Disseminate Departmental and external IPWAR-related methods to subordinate organizations.

(4) Identify IPWAR-related methods within the Departmental element to be shared with DOE via the Office of Cyber Security.

DOE ORGANIZATIONS TO WHICH DOE M 205-1.C IS APPLICABLE
(current as of 9/29/03)

Office of the Secretary
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Office of Counterintelligence
Departmental Representative to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
Office of Energy Efficiency and Renewable Energy
Energy Information Administration
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Hearings and Appeals
Office of Independent Oversight and Performance Assurance
Office of the Inspector General
Office of Intelligence
Office of Management, Budget and Evaluation and Chief Financial Officer
National Nuclear Security Administration
Office of Nuclear Energy, Science and Technology
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Secretary of Energy Advisory Board
Office of Security
Office of Worker and Community Transition
Office of Energy Assurance
Office of Electric Transmission and Distribution
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

CONTRACTOR REQUIREMENTS DOCUMENT

DOE M 205.1-C, *Incident Prevention, Warning, and Response (IPWAR) Manual*

This Contractor Requirements Document (CRD) establishes the requirements for Department of Energy (DOE) contractors, including National Nuclear Security Administration contractors, with access to DOE information systems. Contractors must comply with the requirements listed in the CRD.

This CRD supplements requirements contained in the CRD for DOE O 205.1, including requirements for cyber resource protection, risk management, program evaluation, and cyber security plan development and maintenance. The contractor will ensure that it and its subcontractors cost effectively comply with the requirements of this CRD.

The contractor must ensure that all information systems used by its employees or facilities under its control satisfy, or comply with, the requirements listed below.

1. Categorizing Cyber Security Incidents and Attempted Incidents. Cyber security incidents must be characterized and categorized according to their potential to cause damage to information and information systems based on two criteria: incident type and system category.[1] The criteria are used in combination to determine the time frame for reporting incidents to the Computer Incident Advisory Capability (CIAC). This Manual establishes two incident types (type 1 and type 2) and three categories of system impact (low, moderate, and high), which are described below.

   a. Incident Types.

      (1) Type 1 incidents are successful incidents that potentially create serious breaches of DOE cyber security or have the potential to generate high-visibility media interest. Following are the type 1 incidents currently defined (see also Attachment 4, Definitions).

         (a) *Compromise/Intrusion*. All instances of system compromise or intrusion by unauthorized persons must be reported, including user-level compromises, root (administrator) compromises, and instances in which users exceed privilege levels.

         (b) *Web Site Defacement*. All instances of a defaced Web site must be reported.

         (c) *Malicious Code*. All instances of successful infection or persistent attempts at infection by malicious code, such as viruses, Trojan horses, or worms, must be reported.

[1] The security categorization of systems established by this Manual is based on Federal Information Processing Standards Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, May 2003 (Initial Public Draft).

(d) *Denial of Service*. Denial of service (successful or persistent attempts) that affects or threatens to affect a critical service or denies access to all or large portions of a network must be reported. Critical services are determined by the Heads of Departmental elements.

(e) *Critical Infrastructure Protection (CIP)*. Any activity that adversely affects an asset classified as CIP must be reported. CIP assets are determined by the Heads of Departmental elements.

(2) Type 2 incidents are attempted incidents that pose potential long-term threats to DOE cyber security interests or that potentially degrade the overall effectiveness of the Department's cyber security. Following are the type 2 incidents currently defined.

(a) *Attempted Intrusion*. A significant and/or persistent attempted intrusion is an exploit that stands out above the daily noise level and would result in unauthorized access (compromise) if the system were not protected.

(b) *Reconnaissance Activity.* Persistent surveillance probes and scans are those that stand out above the daily noise level and represent activity that is designed to collect information about vulnerabilities in a network. Departmental elements must determine the standard for collecting data on surveillance probes and scans by subordinate sites.

(c) *Unauthorized Use*. Computer is used for anything but its intended purpose (that is, information is obtained without permission or the system is used to gain access to DOE data without proper permissions).

b. System Category. System categories refer to the impact that an incident could have on Departmental operations (including mission, functions, image, or reputation), Departmental assets, or individuals (including harm to privacy rights) based on the sensitivity of the system and the data it stores, processes, or transmits. This categorization translates into a level of risk associated with the potential loss of confidentiality, integrity, or availability of the system and/or the data stored, processed, or transmitted by the system.

(1) Low Risk. Loss of system confidentiality, integrity, and availability could be expected to have a limited adverse effect on Departmental operations, assets, or individuals, requiring minor corrective actions or repairs.

(2) Moderate Risk. Loss of system confidentiality, integrity, and availability could be expected to have a serious adverse effect on Departmental

operations, assets, or individuals, including significant degradation or major damage, requiring extensive corrective actions or repairs.

(3) High Risk. Loss of system confidentiality, integrity, and availability could be expected to have a severe or catastrophic adverse effect on Departmental operations, assets, or individuals. The incident could cause the loss of mission capabilities for a period that poses a threat to human life or results in the loss of major assets.

2. Reporting Cyber Security Incidents. Guidelines for determining the type of reporting must be documented in the Departmental element Program Cyber Security Plan (PCSP).

a. When a cyber security incident has occurred or is suspected to have occurred, the affected site will immediately examine and document the pertinent facts and circumstances surrounding the incident. (Note: The evidence-gathering period must not exceed 24 hours.)

b. Once the preponderance of evidence indicates an incident has occurred, the incident must be cataloged according to incident type and category of system affected and reported to CIAC within the time frames indicated in Table 1, in accordance with the process established by the Departmental element.

c. If it is determined that an incident did not occur, no further action is required.

Table 1. Required Time Frame for Reporting Cyber Security Incidents to the Computer Incident Advisory Capability

	System Category		
Incident Type	**Low**	**Moderate**	**High**
Type 1	Within 4 hours	Within 1 hour	Within 1 hour
Type 2	Within 1 week	Within 24 hours	Within 24 hours

d. The site must issue a monthly report whether or not it has not experienced any reportable successful or attempted cyber security incidents during the previous month. The reporting process documented in the Departmental element's PCSP should be followed. (Must be checked against PCSP requirements to make sure reporting requirement is documented.)

e. Departmental elements or subordinate organizations must inform the Office of Inspector General of attacks or activities—including persistent attempts at unauthorized access, malicious code, and denial-of-service events—if there is reason to suspect that the attacks/activities are significant, if the attacks/activities are unusually persistent, or if the attacks/activities appear to constitute criminal

activity. Reporting this information to the Office of Inspector General must be done according to the procedures in the PCSP of the Departmental element.

(1) A guideline to help determine whether such events are significant can be found at http://cio.doe.gov/cyberhome/sigguideline.htm.

(2) A guideline to help determine whether such events constitute criminal activity can be found at http://cio.doe.gov/cyberhome/crimguideline.htm.

f. Automated systems may be used for reporting if reporting by such systems complies with the requirements of this Manual.

3. Cyber Alerts.

a. CIAC is the official DOE point of contact for prompt dissemination of information provided in alerts received from external organizations. In addition, CIAC provides Departmental responses to national centers, as required. The timing of distribution will be commensurate with the significance of the information.

b. If CIAC issues an alert, the security points of contact will:

(1) acknowledge the receipt of the alert within 4 business hours; and

(2) execute the required analyses and corrective actions and report the actions taken in accordance with the Departmental element's PCSP.

4. Updating Cyber Security Patches. Security patches must be installed regularly and in a timely manner to help prevent intrusions. (Patches can be obtained from a number of sources, including CIAC, the FedCIRC Web site, and trusted vendors.)

5. Cyber Security Incident Preparedness/Response and Contingency Plans. Because of the interrelationship of cyber security incident preparedness/response and continuity of operations, IPWAR procedures should be integrated into, and tested periodically with, the Departmental elements' information system contingency plans. Contingency plans should include a description of or reference to the IPWAR procedures that would be followed to ensure that the system will continue to have incident protection if a disaster occurs.

6. Cyber Security Incident Training. Departmental elements must ensure that users, system administrators, and cyber security staff are well-versed in IPWAR procedures through initial and annual refresher computer security awareness training.

SITE FACILITY CONTRACTORS TO WHICH THE CRD IS INTENDED TO APPLY
(Current as of 9/29/03)

Facility	Contractor
Management and Operating—*Research*	
Lawrence Berkeley National Laboratory	University Of California
Pacific Northwest National Laboratory	Battelle Memorial Institute
Brookhaven National Laboratory	Brookhaven Science Associates
Sandia National Laboratories	Lockheed Martin - Sandia Corp.
National Renewable Energy Laboratory	Midwest Research Institute
Stanford Linear Accelerator Center	Stanford University
Bettis Atomic Power Laboratory	Bechtel Bettis Inc
Argonne National Laboratory	University Of Chicago
Idaho National Engineering & Environmental Laboratory	Bechtel B&W Idaho LLC
Thomas Jefferson Nat'l Accelerator Facility	Southeastern Universities Res. Assoc.
Ames National Laboratory	Iowa State University
Oak Ridge National Laboratory	University of Tennessee/Battelle
Knolls Atomic Power Laboratory	Lockheed Martin-KAPL, Inc
Lawrence Livermore National Laboratory	University Of California
Los Alamos National Laboratory	University Of California
Savannah River Site	Westinghouse Savannah River Company
Princeton Plasma Physics Laboratory	Princeton University
Fermi National Accelerator Center	Universities Research Association
Management and Operating—*Plant/Facility*	
West Valley Project	Westinghouse-West Valley Nuc. Services
Strategic Petroleum Reserve	Dyn McDermott Petroleum Ops. Co.
Oak Ridge Y-12 National Security Complex	BWXT Y-12 LLC
Pantex Plant	BWXT Pantex LLC
Waste Isolation Pilot Plant	Westinghouse TRU Solutions
Nevada Test Site	Bechtel Nevada Corp
Kansas City Plant	Honeywell Federal Manufacturing & Tech.
National Civilian Radioactive Waste Program (Yucca Mountain)	Bechtel SAIC

Facility	Contractor
Site Restoration	
Hanford Environmental Restoration	Bechtel Hanford Inc
Oak Ridge Environmental Management	Bechtel Jacobs Co LLC
Mound Environmental Management Project	CH2M Hill Mound, Inc
Project Hanford	Fluor Daniel Hanford, Inc
River Protection Project Tank Farm Management	CH2M Hill Hanford Group
Rocky Flats	Kaiser Hill Co. LLC
Fernald Environmental Management Project	Fluor Fernald Inc.
Other	
Grand Junction Technical & Remediation Services	MACTEC Inc.
Grand Junction Facilities & Operations Services	Wastren Inc.
Oak Ridge Institute of Science & Education	Oak Ridge Associated Universities
Occupational Health Services at the Hanford Site	Hanford Environmental Health Foundation

DEFINITIONS

The following terms are specific to the DOE Classified and Unclassified Cyber Security Program. Some definitions are followed by a citation indicating the source. (Citations are given in full on first use and are abbreviated thereafter.) Where no citation appears, the definition has been derived from several sources or from common usage. Many definitions are from the National Security Telecommunications and IT Investments Security Committee's National Information Technology Investments Security (INFOSEC) Glossary. Other definitions may be found in the DOE *Safeguards and Security Glossary of Terms*, which is available online at http://www.directives.doe.gov/pdfs/nnglossary.

Accreditation—Formal declaration by a Designated Accrediting Authority (DAA) that an IS is approved to operate in a particular security mode at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.

Audit—Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Alert—A time-critical message or posting to notify organizations that they are in imminent danger of attack. Alerts require acknowledgment of receipt by the DOE element's primary or alternate point of contact within 4 business hours of successful delivery. The designation "alert" is used for notifications about attacks at other DOE sites, Federal Agencies, or organizations. When a Computer Incident Advisory Capability (CIAC) alert is issued, DOE elements and contractors are requested to review activities at their respective sites for the actions or events described in the alert and provide appropriate notifications if similar activities are found.

Certification—Comprehensive evaluation of the technical and nontechnical security safeguards of an IS to support the accreditation process that establishes the extent to which a particular design and implementation meet a set of specified security requirements.

Classified information—Information that has been determined pursuant to Executive Order 12958 or any predecessor Order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.

Compromise—An incident resulting in the loss of data, data integrity, data confidentiality, and/or system control to any network resource (PC, router, server, firewall, etc.).

Critical Infrastructure Protection (CIP) Asset—Those infrastructure resources listed in an Agency's CIP inventory under Project Matrix.

Cyber Security—The protection of information technology investments against unauthorized access to or modification of information, whether in storage, processing, or transit; against loss

of accountability for information and user actions; and against the denial of service to authorized users, including those measures necessary to protect against, detect, and counter such threats.

Cyber Security Incident—Any adverse event that threatens the security of information resources, including loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability. Adverse events include, but are not limited to, attempts (successful or persistent) to gain unauthorized access to an information system or its data; unwanted disruption or denial of service; unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent. Examples include insertion of malicious code (for example, viruses, Trojan horses, or back doors), unauthorized scans or probes, successful or persistent attempts at intrusion, and insider attacks.

Denial of service—Type of incident resulting from any action or series of actions that prevents any part of an IS from functioning.

Departmental Elements—First-tier Federal organizations at Headquarters and in the field. First-tier entities at Headquarters are the Secretary, Deputy Secretary, Under Secretary, and Secretarial Officers (Assistant Secretaries and Staff Office Directors). First-tier entities in the field are managers of the Operations Offices, managers of the Field Offices, and the administrators of the Power Marketing Administrations.
Headquarters and field elements are described as follows.

- *Headquarters elements* are DOE organizations located in the Washington, D.C., metropolitan area.

- *Field elements* is a general term for all DOE elements (excluding individual duty stations) located outside of the Washington, D.C., metropolitan area.

DOE Contractor—An entity that receives an award from DOE, including management and operating contractors who manage, operate, or provide Departmental element services to DOE research or production facilities that are principally engaged in work for DOE.

DOE Organization—A Headquarters element or subordinate organization including both DOE Federal and DOE contractor entities.

Heads-Up Notice and/or Bulletin—A routine message identifying vulnerabilities and recommended fixes.

Information system (IS)—Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information.

Intrusion Detection—The logging and auditing capability that provides evidence that an attempted or actual breach of protection mechanisms or access controls has occurred.

Malicious code—Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an IS.

National Security System—Any telecommunications or information system operated by the United States Government, the function, operation, or use of which: 1. involves intelligence activities; 2. involves cryptologic activities related to national security; 3. involves command and control of military forces; 4. involves equipment that is an integral part of a weapon or weapon system; or 5. is critical to the direct fulfillment of military or intelligence missions and does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (Title 40 U.S.C. Section1452, Information Technology Management Reform Act of 1996.)

Nonrepudiation—Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

Persistent Incident—A consistent and continual attack on an asset that is determined by the Departmental element or subordinate organization, in accordance with its governing Program Cyber Security Plan (PCSP), to be above the daily noise level and deserving of attention (that is, because something makes the incident stand out from other activity as something that requires attention or investigation).

Risk management—Process of identifying and applying countermeasures commensurate with the value of the assets protected based on a risk assessment.

Significant Incident—Detected activity that deviates from the expected behavior of users of the system that is different from known signature attacks or an activity that stands out from the daily noise level and that the Departmental element or subordinate organization determines, in accordance with its governing Program Cyber Security Plan (PCSP), to require attention or investigation.

Threat— Any circumstance or event with the potential to adversely impact an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. For example,

- External security threats, which come from individuals who use technical knowledge or social engineering to gain unauthorized access (either via remote or gained local access) to perform malicious activity in cyber systems.

- Insider security threats (whether intentional or unintentional) with potential to be more serious than an external threat because the perpetrator of malicious activity has authorized access to the system.

- Foreign access threat (either remote or internal) to the information environment, requiring assessment to ensure that access by foreign nationals to DOE cyber systems is approved

by an official designated by the DOE site manager or line-level organization accountable for the approval decision.

- Portable electronic devices, including laptop computers, palm devices, and cell phones capable of receiving, storing, or transmitting data in an electronic format. Issues of concern include data aggregation, theft, and radio frequency/infrared interconnectivity.

Mosaic threat that classified information or information requiring enhanced protection will be derived by combining open source information made separately available, perhaps by different organizations.

Unclassified— Information that has not been determined pursuant to E.O. 12958 or any predecessor order to require protection against unauthorized disclosure and that is not designated as classified.

Vulnerability— Weakness in an IS, system security procedures, internal controls, or implementation that could be exploited, as follows.

- major vulnerability—if discovered and exploited, could reasonably be expected to result in a successful attack causing serious damage to the national security.

- unspecified major vulnerability—a weakness in a system or organization's defenses that could be exploited and is specified in no greater detail than the specific security system (or one of its major components) when it occurs.

Web Site Defacement. An incident resulting in the loss of data or data integrity to a Web server that could result in misinformation to Departmental customers and collaboration partners, Departmental embarrassment, or the total loss of service.

ACRONYMS

CIO	Chief Information Officer
CIAC	Computer Incident Advisory Capability
CIP	Critical Infrastructure Protection
CIRT	Computer Incident Response Team
CRD	Contractor Requirements Document
CSMP	Cyber Security Management Program
CSPP	Cyber Security Program Plan
FedCIRC	Federal Computer Incident Response Center
FISMA	Federal Information Security Management Act
IPWAR	incident prevention, warning, and response
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PCSP	Program Cyber Security Plan
SP	Special Publication

SAMPLE CYBER INCIDENT RESPONSE PLAN

This sample plan consists of three sections. The first section details the plan's scope, the second describes establishment of roles and responsibilities regarding the Computer Incident Response Team (CIRT), and the final section presents a formal set of procedures for reporting and handling information technology (IT) security incidents. The cyber incident response plan should be included or referenced in the Departmental element's Program Cyber Security Plan document.

1. PLAN SCOPE. Before starting to develop the plan, the Departmental element should determine what the plan will cover and the personnel responsibilities as this will affect the procedures and processes used to handle a computer security incident. The Departmental element should also consider any external connections, including how an incident might affect another Agency, contractor, or Departmental element that is connected in some way to the affected system or network. The Departmental element also should state within the plan how the organization works with its IT and security staffs and the types of systems the plan will cover. This will help determine which job positions the incident response team will need to include.

2. COMPUTER INCIDENT RESPONSE TEAM. The organization's written procedures must identify who will perform the procedures. Accordingly, the response plan should describe the makeup and roles and responsibilities of the CIRT. Depending on the size and structure of the Departmental element, multiple tiers of CIRTs may be required to effectively address incidents, both across the organization and within subordinate organizations. In such cases, the membership of each team should be consistent with competencies appropriate to the team's tier. The team should be composed of a core group, which will be involved in all incidents, and a group of platform and system specialists, who will participate as incidents require.

    a. The Core Group. The core group members include the IT security program manager (or the information system (IS) security manager); representatives from the Inspector General's (IG's) office, public relations (PR), and human resources or personnel; and someone with an investigative or forensics background. The organization can add personnel to the core group as needed.

        (1) *IT Security Program Manager*. This person is the overall head of the organization's IT security program and should be the CIRT leader. In most cases, he or she will appoint someone to be the IS security manager, who will run the day-to-day incident response team operations. This leaves the security program manager free to manage the organization's overall IT security. In the case of a multitier organizational structure, an IS security manager, who will lead the local incident response team, should be appointed for each subordinate organization. As the team leader, the IT security program manager or IS security manager will be the

director of each incident investigation. He or she will decide whether additional personnel are required for an investigation, ensure that all procedures are followed, and decide whether outside assistance is required, as approved by upper management. The IT security program manager also authorizes the release of any information about the incident, again, with upper management consent. However, he or she is not the organization's media spokesperson.

(2) *Inspector General Representative*. The CIRT requires an IG representative who is knowledgeable about the various laws that deal with IT security and privacy. This person's function is to ensure that the team does not violate the law while investigating the incident. The legal representative should also know whom to contact at the local, state/province, and national levels (in the United States, for example, it is the FBI/National Infrastructure Protection Center), and at international law enforcement agencies. The IG representative should be the contact with these law enforcement agencies.

(3) *Public Relations Representative*. PR should be centralized, with information being released only by the Department's PR office. The PR representative is the sole point of contact for the media for release of information, as authorized by the IT security program manager.

(4) *Human Resources or Personnel Representative*. There are various reasons for including a human resources/personnel representative on the team. This person should ensure that the team does not violate employees' rights (for example, privacy) during investigations. In addition, this representative should make sure that appropriate disciplinary methods are used if an employee is found to be the source of an incident.

(5) *IT Investigative/Forensic Expert*. The IT investigative/forensic expert should ensure that the investigation is performed in a methodical manner and that evidence is collected and stored properly. This expertise will assist in the overall handling of the incident and will be especially helpful if the organization wishes to prosecute the individual responsible for the incident. If a prosecution is pursued, the evidence must be collected and handled so that it can be used in the criminal case. This proper handling includes keeping the chain of evidence clean, secure, and verifiable.

b. Incident-Specific Team Members. Other personnel may be added to the CIRT team on an as-needed basis. Although the requirement for additional personnel will depend on the specific incident to be handled, all such personnel must be knowledgeable about the system under attack. Key personnel include the IS security officer, system administrators, communication specialists, system

developers, database administrators, and the system owner. Other personnel may also be included.

(1) *IS Security Officer*. Each general support system or major application should be assigned an IS security officer who ensures that the system is in line with the organization's IT security policy and guidelines. This officer assists the core group in handling an intrusion by stating how the entire system should be set up and configured.

(2) *System Administrators*. System administrators who administer the hardware on which the system runs are critical in incident handling, because of their intimate knowledge of the system hardware, the operating system configuration, and the services that run on the system.

(3) *Network Specialists*. These specialists are essential members of an incident response team because of their knowledge of the network and its configuration, including the firewall configuration if a firewall is used. They will know where a compromised system is connected to the network and whether it has any other connections to the Internet that are not protected by the firewall. They also know how the routers, bridges, and gateways are configured and where they are located within the network. In most cases, these specialists also monitor the intrusion detection system, if the organization uses one.

(4) *System Developers*. System developers know the intricacies of the system or application. Therefore, they know whether the compromised system or application is not running properly and whether it has been modified.

(5) *Database Administrators*. If the compromised system uses a database, database administrators must evaluate whether changes have been made to the database structure or configuration. They can also determine whether any database-specific programs (for example, stored procedures or queries) have been modified.

(6) *System Owner*. It is important that the system owner be part of the incident handling team for several reasons. First, because the owner knows exactly how critical the system is to the organization's mission, he or she can determine how soon an intrusion session should be terminated and whether the system should be taken off the production server. The owner also knows whether a backup system must be put into production immediately or if the system can be kept down until the main system is validated and any system vulnerabilities are corrected. Finally, the system owner knows the proper data format and can tell if the data makes sense and provides the proper output.

c. Response Team Duties. The function of the CIRT is to handle information security incidents as they occur, following the procedures of the IT security program. If an incident occurs, the team members ensure that it is handled as quickly as possible and that it does not affect the security of other systems and applications. In addition, if there is an incident, they should know whom to contact, even if only for informational purposes. The response team also should have procedures for controlling the release of information within the organization.

3. INCIDENT REPORTING PROCEDURES. A standard process for reporting incidents should be developed as part of the formal reporting procedures. This process should include a standardized form that can assist personnel in reporting a suspected computer-related incident. The form should provide the following information:

- name of organization;
- contact information for this incident;
- physical location of affected computer/network;
- date incident occurred;
- time incident occurred;
- which critical infrastructure was affected;
- type of incident (for example, intrusion, denial of service, Web site defacement);
- IP address of affected system;
- IP address of apparent attacker;
- operating system of affected host;
- functions of affected host;
- number of hosts affected;
- suspected method of intrusion/attack;
- suspected perpetrators and/or possible motivations;
- evidence of spoofing;
- system or software affected;
- what security infrastructure was in place;
- whether the intrusion resulted in loss of sensitive information;
- whether the intrusion damaged the system;
- what actions have been taken;
- with whom the information can be shared (for example, National Infrastructure Protection Center, National Security Incident Response Center);
- whether the local FBI office has been informed of the intrusion;
- whether any other agency has been informed, and if so, what its contact information is; and
- last time the system was modified or up.

The incident reporting procedures should stipulate to whom the reporter should send the completed incident reporting form.

4. INCIDENT HANDLING PROCEDURES. Once an incident has been reported, the procedures should stipulate how it should be investigated and handled. These procedures should reflect the requirements of Federal legislation, Office of Management and Budget memorandums and circulars, and National Institute of Standards and Technology standards. The procedures should also implement the processes and requirements identified in draft DOE M 205.1-C, *Incident Prevention, Warning, and Response (IPWAR) Manual,* XX-XX-03, and other applicable DOE policy.

Sample, "At A Glance," Incident Signs and Reporting Worksheet

DOE promotes the education and awareness of all users to the threat posed by unauthorized disclosure of information. This attachment provides sample information that can be distributed to users during awareness training that they can take back to their desks and retain. The signs list helps to promote ongoing awareness of activities that may be disregarded as simple system errors which actually point to a potential incident.

Signs of an incident

You may be able to reduce the impact of an incident across your organization by reporting suspicious or anomalous events as soon as they are detected. While these events don't always involve a security incident they may. If you see multiple events occurring simultaneously you may want to alert the help desk or your supervisor. Common system areas and corresponding abnormal events include:

· Unexplained modification or deletion of data
· Unexplained discovery of new files or unfamiliar filenames
· Multiple unsuccessful and unexplained logon attempts or your account locked
· Unauthorized creation of new user accounts
· Unexplained or suspicious system entries
· Missing or unusually full system logs
· Attempts over a period of time targeted against a specific location (historical analysis)
· Unauthorized modification of file lengths and/or dates
· Unauthorized or unexplained attempts to write to system files or alter system files
· Activation of a system alarm or similar indication of an intrusion
· Denial of service attack on the system
· Multiple users logged on to a single account
· Entire system crashes
· Unauthorized operation of a program, known as a "sniffer device," to monitor network traffic
· Usage of attack scanners or remote requests for information about systems and/or users
· Unusual network activity after normal operating hours
· Abnormal number of locked accounts
· Unauthorized scans of ports or unusually heavy traffic to a specific port

The do and don't lists provided below are examples of those that a Departmental element might use in developing their user incident action and reporting checklist. This list is provided as an example and starting point for the Departmental elements to use in developing and sharing ideas for a comprehensive user checklist.

DO

• Remain calm. Take your time and follow all steps to handle the incident properly.

• Keep detailed notes. Take step-by-step notes and write down observations with times of occurrence as the incident response progresses.

• Leave the system as is! For investigative forensic purposes, it is imperative that the system remains in the same condition as when the incident was discovered. Leave the system in operation until appropriately trained law enforcement personnel can respond.

• Report immediately. Contact your local information security office (ISO) for guidance. You may also contact DOE CIAC at:

DOE-CIAC Web Site	http://www.ciac.org/ciac
DOE-CIAC E-mail	ciac@ciac.org
DOE-CIAC Hotline	925-422-8193
STU-III Phone	925-423-2604

In an emergency you many also contact FedCIRC: www.fedcirc.gov or (888) 282-0870

• Notify the appropriate individuals. Management should be informed so proper decisions can be made.

• Prepare to find more than you are looking for. You never know what you may find when looking at an employee's computer that could lead to evidence of other computer crimes.

DON'T

• Rush! Trying to respond too quickly may cause unnecessary mistakes to be made.

• Power down the machine. Valuable information regarding the incident could be lost.

• Use a video camera. It may disclose agency-sensitive information if the case is taken to court.

• Wait to respond. Waiting to respond can cause evidence to be lost, and staff may forget details to answer important questions.

• Run/install programs on the system. This could overwrite potential evidence on the system.

• Underestimate the incident scope. If you underestimate the scope of the incident, you may miss crucial evidence.

- Keep information from the decision makers. If management lacks the necessary information to make informed decisions, the response may not be handled in the most effective manner.